Procedure No 2205.04 Acceptable Encryption Policy
Reference: Policy No. 2205
Effective Date: 12/28/04
Prior Issue: N/A

Purpose:

The Arizona Department of Juvenile Corrections (ADJC) Management Information Systems (MIS) provides standards that limit the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. The standards also provide direction to ensure that Federal regulations are followed, and that legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Rules:

1. **USERS** shall use proven, standard algorithms such as AES, DES, Blowfish, RSA, WEP, RC5 as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.

2. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. **MIS** shall review ADJC's key length requirements annually and upgrade as technology allows.

3. **USERS** shall not use proprietary encryption, unless reviewed by qualified experts outside of the vendor in question and approved by Government Information Technology Agency (GITA**)**. The export of encryption technologies outside of the United States is restricted by the U.S. Government and punishable by Federal Guidelines.

4. **MIS** shall make use of the 802.1x security standards for **USERS** having centralized user authentication and automated key distribution with standard wireless networks (IEEE 802.11x for LAN and IEEE 802.16 for MAN):
   a. Per GITA P800-S830, the IEEE 802.11 standard that defines Wired Equivalent Privacy (WEP) specifies a 40-bit and 128-bit encryption key, both of which are unacceptably susceptible to compromise;
   b. Once developed, the IEEE 128-bit encryption solution, Enhanced Security Network (ESN), shall be used for wireless networks.

5. **MIS** shall make available to ADJC employees and other State Agency's the ability to use encryption schemes to protect electronic information conducted outside of ADJC's network per GITA P800-S850. This is including but not limited to:
   a. Email;
   b. Remote access;
   c. Inter-agency service extensions.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: